Summer Examinations 2011

Exam Codes	4BS1, 4CS1
Exams	4th Science
Module	Rings and Fields
Module Code	MA416 and MA491
External Examiner	Dr C. M. Campbell
Internal Examiner(s)	Dr G. J. Ellis Dr K. E. G. Sköldberg Dr J. J. J. Ward
Instructions:	**In Section A, answer Question A1 and one of questions A2 and A3.** **In Section B, answer Question B1 and one of questions B2 and B3.**
Duration	3 Hours
No. of Pages	3 pages, including this one
Department	School of Mathematics, Statistics and Applied Mathematics
Requirements:	No special requirements
Release to Library:	Yes

Section A – Ring Theory (MA416)

A1. Answer seven of the following ten parts.

(a) Decide whether each of the following is a ring. In each case, if you believe that the object *is* a ring, it is enough to just say so. If you believe that the object is *not* a ring, you should give a reason why the object is not a ring.

i. The set of *antisymmetric* 2×2-matrices with entries in $\mathbb{Z}$, under the usual addition and multiplication of matrices. (A matrix is antisymmetric if $A^{\mathrm{T}} = -A$).

ii. The set of polynomials p in $\mathbb{R}[x]$ such that $p(0) \neq 0$ under the usual addition and multiplication of polynomials.

iii. The set of complex numbers that can be written in the form $p + qi$ where $p, q \in \mathbb{Q}$ and $i^2 = -1$.

(b) What does it mean to say that an element in a ring R is a *unit* of R? Show that the set of units in R form a group, and give an example of a ring with infinitely many units, and an example of a ring with exactly two units.

(c) Let R be a commutative ring. What is meant by a zero-divisor of R? Show that a unit in R cannot be a zero-divisor, and give an example of an element in a commutative ring which is neither a unit nor a zero-divisor.

(d) Give the definition of a *primitive* polynomial in $\mathbb{Z}[x]$ and show that the product of two primitive polynomials is again primitive.

(e) What is meant by a *field*? Give an example of a field with finitely many elements. Show that if α is a root of the polynomial $p(x) \in F[x]$ then $x - \alpha$ divides $p(x)$.

(f) Determine, with explanation, whether each of the following polynomials is irreducible in the indicated ring:

i. $x^4 + 8x^3 + 12x^2 - 18$, in $\mathbb{Z}[x]$.

ii. $x^5 + 3x^2 - 7x - 1$ in $\mathbb{R}[x]$.

iii. $x^3 - x^2 - 2$ in $\mathbb{Z}_5[x]$.

iv. $2x^3 - x^2 + 1$ in $\mathbb{Q}[x]$.

(g) Let R and S be commutative rings. What does it mean to say that a function $\varphi : R \longrightarrow S$ is a *ring homomorphism*? If $\varphi : R \longrightarrow S$ is a ring homomorphism, define the *kernel* of φ, and show that it is an ideal of R. If $\varphi(r)$ is a unit in S, does it follow that r is a unit in R?

(h) Let R be a commutative ring. What is meant by an *ideal* of R? What is meant by a *principal ideal* of R? Show that every ideal in $\mathbb{Q}[x]$ is principal, and give an example of a non-principal ideal in a ring.

(i) Suppose that R is a commutative ring, and that I is an ideal in R. Let $a + I$ and $b + I$ be two cosets of I in R. Show that $a + I = b + I$ if, and only if $a - b \in I$. Give the definition of multiplication in the quotient ring R/I, and show that it is well defined.

(j) Let R be a commutative ring. What is meant by a *maximal ideal* in R? What is meant by a *prime ideal* in R? Show that every maximal ideal is prime, and give an example of a non-maximal prime ideal in a commutative ring.

A2. (a) Give the definitions of the concepts *Principal Ideal Domain* and *Euclidean ring*.

(b) Show that every Euclidean ring is a principal ideal domain.

(c) Show that in a Euclidean ring, $d(a) = d(1)$ if and only if a is a unit. Hence, or otherwise, characterise the units in the ring of Gaussian integers $\mathbb{Z}[i]$.

A3. (a) State and prove *Eisenstein's irreducibility criterion*.

(b) Prove that the polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$ if p is prime.

Section B – Field Theory (MA 491)

B1. Answer **seven** of the following nine parts. Each part is worth 4 marks.

(a) Explain how a field $\mathbb{K}$ may be viewed as a vector space over a sub–field $\mathbb{F}$ and hence define the **degree** $[\mathbb{K} : \mathbb{F}]$.

(b) Determine the degree of the extension $[\mathbb{Q}\left(\sqrt{11+6\sqrt{2}}\right) : \mathbb{Q}]$.

(c) If the degree of u over the field $\mathbb{K}$ is odd, prove that $\mathbb{K}(u) = \mathbb{K}(u^2)$.

(d) Show that $\mathbb{Q}(i,\ \sqrt{2})$ is the splitting field of the polynomial $f(x) = x^4 - x^2 - 2$ over $\mathbb{Q}$.

(e) Verify that $\Phi_8(x)\ (=\ x^4+1)$ factorises (reduces) in $\mathbb{Q}(\sqrt{2}i)$, where $i = \sqrt{-1}$.

(f) Let p be an **odd** prime. Show that $\Phi_{2p}(x) = \Phi_p(-x)$.

(g) Prove that for $n\ \geq 2,\ \ \Phi_n(x)$ is a **reciprocal** polynomial, in that
$\Phi_n(x) = x^k \Phi_n\left(\frac{1}{x}\right)$ where $k = \phi(n)$ is the degree of $\Phi_n(x)$.

(h) State Gauss' Theorem concerning the values of n for which the regular n–gon can be constructed by straight edge and compass.

(i) Show that $\cos^{-1}\left(\frac{23}{27}\right)$ can be trisected using straight–edge and compass.

B2. (i) Let p be a prime. Show that $x^p - 2$ is irreducible over $\mathbb{Q}$.
Prove that the splitting field of $x^p - 2$ over $\mathbb{Q}$ has degree $p(p-1)$.

(ii) Determine the Galois group G of $x^3 - 2$ over $\mathbb{Q}$ and establish that G is non–abelian of order 6.

(iii) Under the Galois correspondence find the (fixed) subfield corresponding to the subgroup of G of order 3.

B3. (i) Let $\mathbb{F}_q$ be a finite field of order $q\ (= p^n,\ p$ a prime $\ n \geq 1)$. State the main properties of $\mathbb{F}_q$.

(ii) Prove Gauss' formula

$$N_q(d) = \frac{1}{d}\sum_{k|d} \mu\left(\frac{d}{k}\right) q^k$$

where $N_q(d)$ is the number of monic irreducible polynomials of degree d over the finite field of order q.

(iii) By factorising $x^{16} - x$ over the field of two elements $\mathbb{F}_2$, or otherwise, determine the irreducible polynomials of degree 4 over the field of two elements $\mathbb{F}_2$.

(iv) Choosing any of the irreducible quartics in part (iii), show that it can be factored into a product of two irreducible quadratics over $\mathbb{F}_4$, the finite field of order 4.